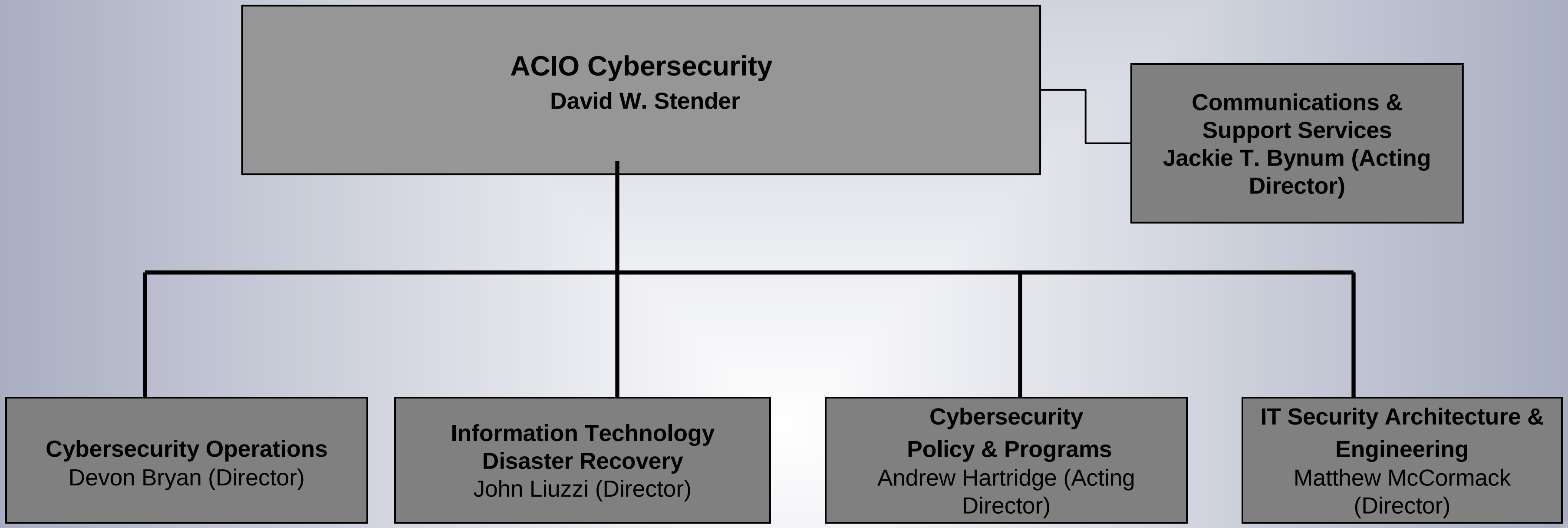
IRS

Modernization Information Technology Services

ACIO Cybersecurity

Teaming for Results

IRS MITS ACIO Cybersecurity Organization



ACIO Cybersecurity
David W. Stender

Communications & Support Services
Jackie T. Bynum (Acting Director)

Cybersecurity Operations
Devon Bryan (Director)

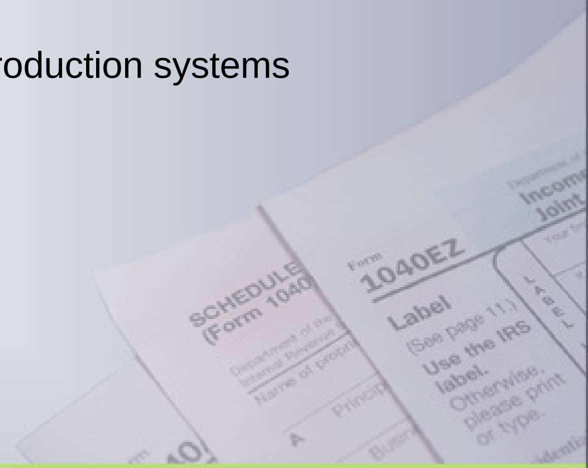
Information Technology Disaster Recovery
John Liuzzi (Director)

Cybersecurity Policy & Programs
Andrew Hartridge (Acting Director)

IT Security Architecture & Engineering
Matthew McCormack (Director)

Cybersecurity: Responsibilities

- Provide management and oversight over the IRS-wide IT security program in accordance with the requirements of FISMA.
- Responsible for:
  - IRS IT security policy and process guidance
  - Systems security certification
  - Systems security testing
  - Security training
  - FISMA compliance reviews
  - Disaster recovery planning, coordination and testing
  - Operation of the computer security incident response center (CSIRC)
  - Lock box and contractor reviews
  - Compliance oversight and systems audits for development and production systems



Cybersecurity: Tasks

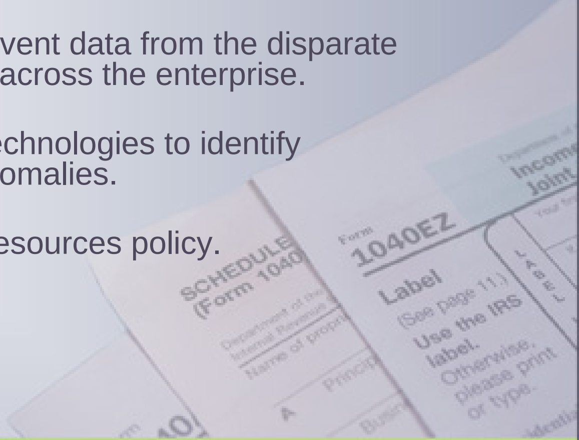
Communications and Support Services

Computer Security Material Weakness

- Perform risk Analysis & Assessment of IRS implementations of technical solutions to resolve CSMW or significant deficiencies in IT security.
- Perform oversight and compliance monitoring that supports eliminating new or repeat findings by GAO audits.

Cybersecurity Incident Response Center (CSRIC):

- **Incident Management -** centralized clearinghouse for incident reporting and analysis of security audit trails.
- **Outreach & Awareness -** collaboration and sharing of information with IRS constituency and external entities.
-
- **Security Notifications -** early warnings and indicators of emerging threats and vulnerabilities applicable to the IRS infrastructure.
- **Vulnerability Analysis & Assessment -** security assessment and penetration testing of enterprise systems to identify vulnerabilities and/or system weaknesses.
- **Security Information Management -** collection, aggregation, and correlation of event data from the disparate information security devices; providing a holistic view of security events occurring across the enterprise.
- **Intrusion Detection/Prevention -** strategic deployment of detection/prevention technologies to identify unauthorized/malicious activity, violations of policy, or other protocol and traffic anomalies.
- **Internet Misuse -** enforcement of IRS' Limited Personal Use of Government IT Resources policy.



Cybersecurity: Tasks

Mainframe Security Support

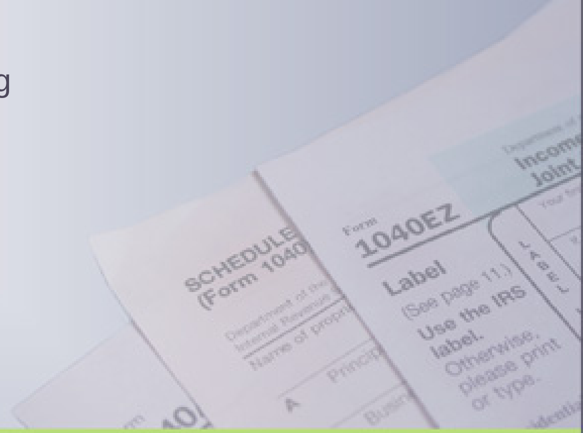
- Perform security reviews to ensure compliance with policy and investigations of information security anomalies to ensure that IRS information systems are used only as authorized by IRS policies. Monitor IT assets through enumeration scans to ensure accurate inventory and remedial actions go back to the DAA for resolution. Review event logs and user activities to identify unauthorized or inappropriate activities or events requiring attention.

Infrastructure Security and Reviews

- Actively work with both internal and external organizations to ensure security requirements are understood and implemented throughout the IRS organization, Lockbox sites, and contractor facilities. We also work with our external stakeholders, including state tax agencies to build partnerships and ensure security requirements are understood.

Information Technology Disaster Recovery

- Business Impact Assessments
- Technical Assessment of IT Infrastructure – Capabilities / Risk / Vulnerability Analyses
- Disaster Recovery Plan Development
- Critical Infrastructure Protection program – Interdependency Analyses
- Disaster Recovery Exercise Coordination and FISMA IT Contingency Plan Testing
- Compliance Monitoring - Material Weakness and Audit Finding Remediation



Cybersecurity: Tasks

Policy and Programs

Security Policy

- Develop and maintain OMB-/NIST-compliant security policy
- Provide guidance and improvements to current practices to ensure effective policy implementation

Certification & Accreditation

- Develop system documentation (e.g. SSP, ITCP)
- Perform security test and evaluation (ST&E) in support of system security certification
- Support DAA Plan of Action and Milestone (POA&M) development and maintenance

FISMA Program

- Manage FISMA-reportable inventory of applications and general support systems (GSS)

Security Strategy and Performance Metrics

- Develop and maintain security program plan
- Develop definition, key design principles and conceptual architecture of identify and access management (IdAM)
- Develop and maintain (FISMA) performance metric tool(s)
- Provide security subject matter expertise (SME) for projects

Cybersecurity: Tasks

IT Security Architecture & Engineering

Security Risk Assessment

- Performing NIST/FISMA based Security Risk Assessments in support of the Enterprise Life Cycle development model.

Security Architecture Support

- Support security architecture by providing subject matter expertise in a wide range of security segments such as wireless networking, SOA, securing web based applications, infrastructure security, secure protocols, advanced encryption algorithms and ad hoc security initiatives.

Advanced Technical Analysis

- Support the ATA organization through secure code analysis and remediation, internal and external penetration testing, ethical hacking, black and white hat testing.